Cryptographic API Requirements for FDIC Financial Applications

Russ Davis

The Challenge

- Multiplicity of Cryptographic APIs
  - GSSAPI
  - CDSA
  - CryptoAPI ...
- High Programmer Turnover Rate
- Vendor Support
- API Integration
  - Too Easy to Make Mistakes
  - Few Understand the Technology

Current Code Issues

- Design Philosophy
  - Tendency to Over Rely on Software Development Tools
  - Non-Portable Vendor Proprietary Solutions
- Commercial Software Bugs
  - Hazard (problem) Avoidance
  - Version Upgrades versus Software Patches
- Application Low Level Calls

High Level API

- High Level API Easier to Understand
  - Commercial API Seen as Too Complex
- Reduced Number of Available Calls
  - Hundreds of Available Calls Were Reduced to a Few
- Used to Avoid Discovered Hazards
  - Calls to Known Software Bugs Prevented

Benefits

- Easier to Code & Test
- Easier to Test Code
- Potential to Provide Portable Applications
  - Government Off The Shelf
- Forces the PKI to do the Heavy Lifting
  - Accommodates Multiple Policies